Caso de estudio de comunicaciones seguras sobre redes móviles ad hoc

Sergio H. Rocabado Moreno[1], Daniel Arias Figueroa[1], Ernesto Sánchez[1], Javier Díaz[2]
[1]C.I.D.I.A. – Centro de Investigación y Desarrollo en Informática Aplicada (UNSa)
[2]L.IN.T.I. – Laboratorio de Investigación en Nuevas Tecnologías Informáticas (UNLP)
[1]srocabad@cidia.unsa.edu.ar, [1]daaf@cidia.unsa.edu.ar, [1]esanchez@cidia.unsa.edu.ar, [2]jdiaz@unlp.edu.ar

Resumen. En este trabajo se presenta el estudio de un caso de integración de una MANET desplegada en zona remota a una red de infraestructura, buscando un equilibrio entre el nivel de seguridad y el consumo de recursos como la energía y el ancho de banda. Se implementaron canales de comunicación extremo a extremo, entre un nodo de la MANET y el servidor de infraestructura. Inicialmente se efectuaron pruebas inyectando tráfico de datos sobre un canal "no seguro", con la finalidad de obtener métricas de referencia como latencia, throughput y consumo de energía. Luego se configuraron canales "seguros" sobre los que se realizaron las mismas pruebas utilizando protocolos como IPSEC y SSL/TLS. Las métricas obtenidas utilizando canales seguros fueron comparadas con las de referencia para determinar las diferencias de consumo de recursos introducidas por la seguridad.

Palabras Clave: MANET, Latencia, Energía, Throughput, IPSec, SSL, TLS, Bluetooth, GPRS.

1. Introducción

Una red móvil ad-hoc o MANET (Mobile Ad hoc NETworks en inglés) [1] es una colección de nodos inalámbricos móviles que se comunican de manera espontánea y autoorganizada constituyendo una red temporal sin la ayuda de ninguna infraestructura preestablecida (como puntos de acceso WiFi o torres de estaciones base celulares) ni administración centralizada.

Por sus características las MANET constituyen una tecnología ideal para facilitar servicios de comunicación a dispositivos móviles en zonas remotas donde no es posible montar y configurar redes de infraestructura debido a inconvenientes físicos y recursos limitados, como la energía y/o cobertura de red celular.

Una ventaja adicional de este tipo de redes es la posibilidad de integrarlas a redes de infraestructura con diferentes fines, entre otros podemos mencionar, el acceso a Internet y a sistemas de información de una intranet desde los dispositivos móviles que forman parte de la MANET. Las características intrínsecas de este tipo de redes (incluyendo autoconfiguración, ausencia de infraestructura, movilidad de los nodos, topología dinámica, ancho de banda limitado, falta de seguridad, conservación de

energía, entre otras), plantean exigencias que deben resolverse antes de realizar la integración [2].

Nuestra investigación se enfoca en los siguientes aspectos:

- **Seguridad**. Las redes móviles utilizan un medio compartido (aire) para transmitir los datos y se encuentran expuestas a "ataques" o accesos no autorizados, y por esta razón se hace necesario utilizar protocolos de seguridad que permitan una integración "segura" de los dispositivos móviles a la red de infraestructura, garantizando el cumplimiento de los siguientes aspectos de seguridad: Confidencialidad, integridad, autenticación y no repudio.
- **Conservación de Energía**. Los dispositivos móviles que conforman la MANET tienen capacidad limitada de energía y pocas posibilidades para recarga de baterías cuando se encuentran en zonas remotas de recursos energéticos limitados, por lo tanto se debe optimizar el consumo de energía.
- **Ancho de banda limitado**. La integración de una MANET en zona remota a una red de infraestructura requiere el uso de la red celular. En este tipo de zonas la cobertura de red celular es muy baja y debido a ello proporciona un ancho de banda reducido y variable.

Los tres aspectos son importantes y están directamente relacionados, se debe tener en cuenta que la implementación de un protocolo de seguridad implica un consumo de energía adicional por tres motivos: 1. Se incrementa el uso de CPU y memoria para realizar cálculos, 2. Se generan encabezados adicionales (overhead) que deben ser transmitidos y 3. Se intercambian mensajes para el establecimiento de canales de comunicación seguros.

Por otra parte, la implementación de niveles de seguridad elevados implica un aumento en el consumo de energía en los nodos móviles que reduce drásticamente el tiempo de vida de la red, y un consumo adicional de ancho de banda que puede comprometer el normal funcionamiento de las aplicaciones. Debido a estas razones se hace necesario establecer un compromiso entre seguridad y consumo de recursos.

En este trabajo se presenta el estudio de un caso de integración de una MANET, desplegada en una zona remota, a una red de infraestructura. El objetivo principal es el de proporcionar, a los nodos de la red ad hoc, acceso "seguro" a un servidor de la red de infraestructura, sin comprometer recursos como ancho de banda y energía que son limitados en la zona de despliegue. Para ello, se implemento un escenario de pruebas que comprende el despliegue de una MANET en zona remota y la integración de la misma a una red de infraestructura a través de la red celular. Sobre el escenario propuesto se establecieron canales de comunicación extremo a extremo, entre un nodo de la MANET y un servidor de infraestructura. Inicialmente, se realizaron pruebas inyectando tráfico de datos sobre un canal "no seguro" para obtener valores de referencia para latencia, throughput y consumo de energía. Luego, se efectuaron las mismas pruebas utilizando canales de comunicación "seguros" configurados sobre protocolos IPSEC y SSL/TLS. Los resultados obtenidos utilizando canales "seguros" fueron comparados con los valores de referencia para determinar las diferencias de consumo de recursos. Las desviaciones que surgieron de estas comparaciones, permitieron:

- Establecer el consumo adicional de recursos generado por el uso de protocolos seguros.

- Realizar un estudio comparativo de rendimiento, entre diferentes configuraciones de protocolos de seguridad.
- Determinar que protocolo seguro se adapta mejor a este tipo de entornos.

2 Trabajos previos del grupo de investigación

En [3], se desplegó un escenario de pruebas *indoor* sin considerar condiciones externas como distancia, interferencias y otras. Se efectuaron mediciones sobre un canal "no seguro" y luego sobre un canal "seguro", el aseguramiento del canal se implemento utilizando diferentes configuraciones del protocolo IPSec en modo transporte (extremo a extremo). En los resultados se presentan gráficos comparativos de consumo de energía entre las diferentes configuraciones de seguridad.

En [4], continuamos con esta línea de investigación, utilizando IPSec para el aseguramiento del canal de comunicaciones, esta vez sobre un escenario de pruebas *outdoor* afectado por factores externos que disminuyen el rendimiento e incrementan el consumo de recursos en los nodos de la red ad hoc. En el desarrollo de la publicación, se fundamenta la elección de Bluetooth como tecnología de soporte para la formación de la MANET remota y de GSM/GPRS para la integración de la misma a la red de infraestructura. Entre los resultados se presentan gráficos que muestran el consumo de energía para cada configuración de canal y la distribución del consumo entre los siguientes ítems: Establecimiento de sesión, encriptación, autenticación y transmisión.

En [5], se describe una experiencia del uso de MANETs en zonas rurales de recursos limitados (energía y ancho de banda). En el trabajo de campo realizado, se desplegaron MANETs de bajo consumo en escuelas rurales, con la finalidad de facilitar a docentes y alumnos el acceso a contenidos m-learning instalados en un servidor de infraestructura. Se consiguió mantener el rendimiento de la MANET dentro niveles aceptables de eficiencia y sin comprometer los recursos, lo que posibilito un funcionamiento correcto de las estrategias de m-learning en este tipo de zonas. Entre las conclusiones de esta publicación se destaca la siguiente: "El uso de las MANETs es efectivo y eficiente para el desarrollo de experiencias de m-learning en zonas de recursos energéticos limitados".

3. Escenario de pruebas

En la Figura 1 se observa la representación gráfica del escenario implementado para realizar las pruebas y mediciones. En el mismo se conecta una MANET, desplegada en zona remota, a la Intranet del campus universitario de la UNSa, a través de la red celular (GSM/GPRS). Los dispositivos móviles (nodos) de la MANET se conectan al servidor "testing" utilizando un canal de comunicación TCP/IP extremo a extremo (end to end). El tráfico entre el nodo móvil y el servidor se gestiona a través de uno de los nodos que actúa como Gateway entre la MANET y la red celular. Este nodo es el encargado de enviar los paquetes de datos hacia los routers de la red celular; desde

donde y a través de Internet son encaminados a la intranet para ser entregados al servidor.

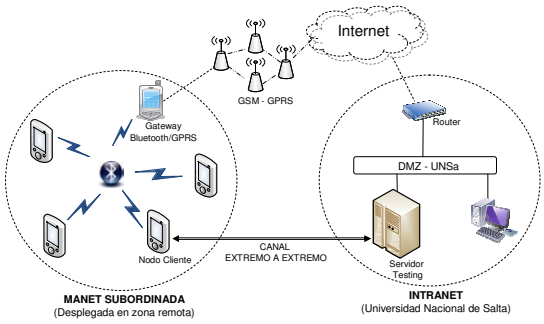

Figura 1. Escenario de pruebas

La conexión del dispositivo móvil cliente al punto de acceso a la red (NAP - Network Access Point) se realizó utilizando el perfil PAN (Personal Área Network) [6] del estándar Bluetooth [7]. El punto de acceso a la red se configuro sobre el nodo Gateway utilizando la funcionalidad "Bluetooth Tethering" de Android, que utiliza el Framework netfilter e iptables para implementar un puente entre la PAN bluetooth y la red GSM/GPRS [8].

El canal de comunicación provee comunicación TCP/IP, extremo a extremo, entre el nodo cliente y el servidor "Testing". En el trayecto los datagramas IP son encapsulados en BNEP [9] por la red Bluetooth y GTP [10] por la red GPRS.

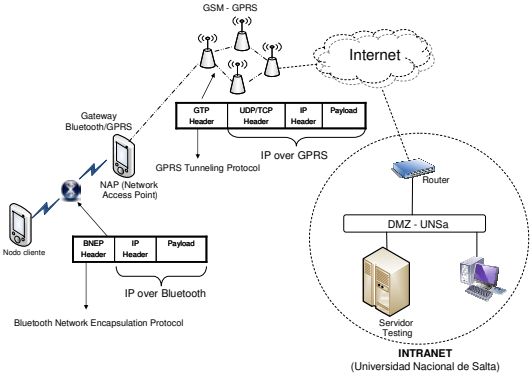

Figura 2. Comunicación extremo a extremo

La Figura 2 ilustra el envío de un datagrama IP desde el nodo móvil hasta el servidor de la intranet siguiendo los siguientes pasos:

1. El nodo móvil envía el datagrama IP, encapsulado en BNEP [9], al punto de acceso a la red (NAP).
2. El NAP transmite el datagrama al SGSN de la red GPRS, desde donde viaja al GGSN encapsulado en GTP [10].
3. El GGSN re-envía el datagrama a Internet, por donde viaja hasta llegar al router frontera de la red destino.

4. El router frontera de la red destino encamina el datagrama hacia el servidor, encapsulado en una trama Ethernet.

3.1 Configuración del nodo cliente

La configuración del dispositivo móvil con el cual se realizaron las pruebas, es la siguiente:

Equipo:	Samsung I9300 Galaxy S III
CPU:	Quad-core 1.4 GHz Cortex-A9
Chipset:	Exynos 4412 Quad
RAM:	1024MB RAM.
SO:	Android OS ver. 4.1.2 (Jelly Bean)
Root:	SI
Bluetooth:	ver 3.0
Bateria:	Lítio-íon, 2100 mAh, 3.7 v.

Este equipo fue especialmente preparado para minimizar el consumo de batería, se procedió entonces a: desinstalar las aplicaciones no indispensables para su funcionamiento, deshabilitar dispositivos de hardware no utilizados en las pruebas y habilitar el modo de bajo consumo.

4. Métricas y aplicaciones elegidas para efectuar las mediciones

Para medir el rendimiento del canal de comunicaciones extremo a extremo, entre el nodo cliente y el servidor, se eligieron las siguientes métricas: Latencia, Throughput y Consumo de energía. En la tabla 1 se muestran las aplicaciones, del lado del cliente y del lado del servidor, que fueron utilizadas para obtener las métricas.

Tabla 1. Aplicaciones utilizadas para obtener las métricas

Métrica	Aplicación Cliente	Aplicación Servidor
Latencia ICMP	Busybox Ping [11]	Windows Stack TCP/IP
Latencia HTTP	HTTPing [12]	HTTP Server (IIS6)
Throughput TCP	Iperf Client [13]	Iperf Server
Throughput HTTP	Busybox Wget [11]	HTTP Server (IIS6)
Throughput FTP	Busybox Wget [11]	FTP Server (Filezilla)
Consumo de energía	Powertutor [14]	----------

5. Configuraciones de canal

Los canales fueron divididos en 2 grupos: 1. Canal no seguro y 2. Canal seguro basado en VPN (L2TP/IPSEC, OPENVPN SSL/TLS y OPENVPN SSL/TLS con compresión LZO). La tabla 2 resume las aplicaciones utilizadas para la implementación de los canales.

Para establecer un canal de comunicación NO seguro, alcanza con brindar transporte IP entre el nodo cliente y el servidor (ver figura 2), mientras que para el establecimiento de canales seguros se requiere el uso de protocolos seguros como IPSec y SSL/TLS.

Tabla 2. Configuraciones de seguridad (Cliente/Servidor)

CANAL	Protocolo seguro	Cliente (Android)	Servidor (Windows)
No seguro	Ninguno	N/A	N/A
Seguro	IPSEC	CLIENTE L2TP/IPSEC	RRAS L2TP/IPSEC
	SSL/TLS	OPENVPN Client [15]	OPENVPN Server [16]
	SSL/TLS/LZO	OPENVPN Client [15]	OPENVPN Server[16]

El canal seguro IPSec se implemento utilizando el protocolo L2TP encapsulado en IPSec [17]. IPSec se configuro en modo transporte utilizando una asociación de seguridad (SA) entre el nodo cliente y el servidor. Elegimos: 1. El algoritmo RSA para la autenticación mutua, entre el nodo cliente y el servidor 2. El algoritmo SHA1 para calcular el código de autenticación de mensaje (MAC), utilizado para verificar la integridad de los mensajes y 3. El algoritmo de encriptación 3DES para la confidencialidad.

El canal seguro SSL/TLS [18] se configuro utilizando la aplicación OPENVPN con y sin compresión LZO [19]. Elegimos: Autenticación RSA de tipo desafío respuesta para el servidor y autenticación RSA para el nodo cliente, HMAC-SHA1 para la integridad y 3DES para la confidencialidad.

La gestión de lo certificados utilizados por los protocolos seguros, fue realizada por una CA montada en el servidor "Testing".

Tabla 3. Protocolos y algoritmos utilizados para la implementación de canales seguros

Canal	Protocolo	Autenticación	Cifrado	Integridad	Compresión
NO Seguro	IP	n/a	n/a	n/a	n/a
Seguro L2TP/IPSEC	IPSEC	RSA (mutual)	3DES (168 bits)	HMAC-SHA1 (160 bits)	n/a
Seguro OPENVPN	SSL/TLS	RSA (Servidor, Cliente)	3DES (168bits)	HMAC- SHA1 (160 bits)	n/a
Seguro OPENVPN	SSL/TLS	RSA (Servidor, Cliente)	3DES (168 bits)	HMAC- SHA1 (160 bits)	LZO

6. Mediciones realizadas

En la tabla 4 se presentan las mediciones efectuadas para cada configuración de canal y el mecanismo utilizado para generar trafico entre el cliente y el servidor.

Tabla 4. Mediciones y mecanismos utilizados

Medición	Mecanismo utilizado para generar tráfico
Latencia ICMP	Echo Request/Reply (32 bytes)
Latencia HTTP	HTTP GET
Throughput TCP y	Inyección de tráfico TCP aleatorio (1024 Kbytes)

consumo de energía	
Throughput HTTP y consumo de energía	Descarga de archivo (de 1024 Kbytes) utilizando HTTP.
Throughput FTP y consumo de energía	Descarga de archivo (de 1024 Kbytes) utilizando FTP.

Las mediciones se realizaron de manera automática, utilizando aplicaciones (figura 3) que se ejecutaron de manera continua durante 7 días en la franja horaria 6:00 am a 11:00 pm, de esta manera fueron contemplados diferentes niveles de carga de la red GPRS. Los resultados obtenidos se promediaron para determinar el valor final de cada medición.

MEDICIONES	CONFIGURACION DE CANAL			
	NO SEGURO	L2TP IPSEC	OPENVPN (SSL/TLS)	OPENVPN LZO (SSL/TLS)
Latencia ICMP (Busybox Ping)	SI	SI	SI	SI
Latencia HTTP (HTTPing)	SI	SI	SI	SI
Throughput TCP (Iperf)	SI	SI	SI	SI
Throughput HTTP (Busybox Wget)	SI	SI	SI	SI
Throughput FTP (Wget - ANDftp)	SI	SI	SI	SI

Consumo de energía (PowerTutor)

Figura 3. Resumen de configuraciones de canal implementadas, mediciones realizadas y aplicaciones utilizadas para medir.

El consumo de energía en el nodo cliente se midió utilizando la aplicación PowerTutor [14], esta herramienta permite estimar el consumo de energía en tiempo real y por proceso utilizando el modelo de consumo de energía descrito en [20] .

6.1 Metodología de medición

A continuación se enumeran los pasos necesarios para efectuar una medición:

- Establecer comunicación extremo a extremo, según la configuración de canal utilizada (ver tabla 3).
- Ejecutar la aplicación Powertutor.
- Arrancar el monitoreo de consumo de energía (“Start Profiler”)
- Generar tráfico entre el Cliente y el Servidor, el mecanismo depende de la medición realizada (ver tabla 4)
- Detener Powertutor (“Stop Profiler”)
- Guardar el “log” de Powertutor (Pulsar Menú -> Save Log).
- Copiar el “log” generado por “Powertutor”.
- Copiar el “log” generado por la aplicación utilizada para la medición.
- Analizar y procesar los archivos de logs.
- Promediar resultados.

7. Resultados

A continuación se presentan algunos de los resultados obtenidos, utilizando gráficos que resumen los aspectos estudiados.

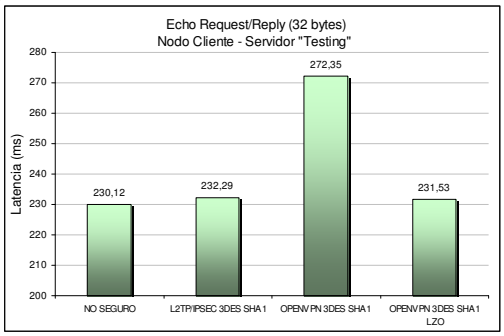

Figura 4. Latencia ICMP echo request/Reply

En la figura 5 se presenta el Throughput alcanzado una descarga de archivo de 1024 Kbytes, utilizando los protocolos HTTP y FTP. Se observa que HTTP alcanza un rendimiento ligeramente superior a FTP en todos los casos.

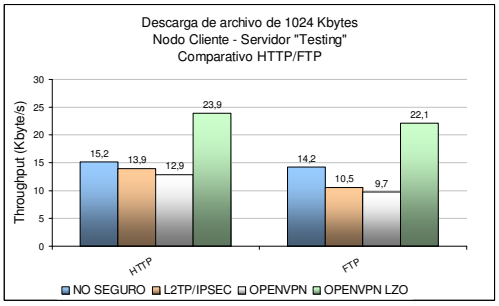

Figura 5. Throughput de descarga HTTP y FTP

El grafico de la figura 6 muestra el Throughput, obtenido por la aplicación Iperf para cada configuración de canal, y la cantidad de energía (en joules) consumida por iperf para efectuar la prueba. Comparando los resultados obtenidos para el canal no seguro y el canal seguro con compresión, se observa que la compresión mejora considerablemente el Throughput (~ 400%) e introduce un consumo adicional de energía (~ 200%).

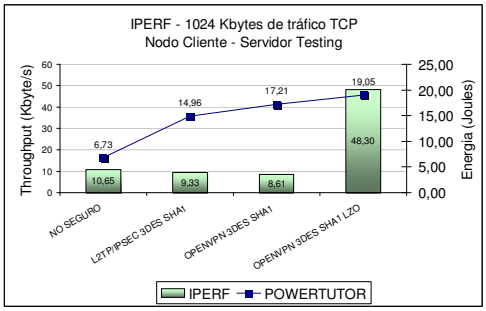

Figura 6. Rendimiento TCP/Iperf (throughput vs energía consumida)

8. Conclusiones y trabajos futuros

La seguridad implica un consumo adicional de recursos que puede variar dependiendo de los protocolos que se elijan para el establecimiento de un canal seguro, en los gráficos comparativos presentados se visualiza que la opción de seguridad basada en SSL/TLS con compresión (3DES - SHA-1 - LZO) es la que mayor energía consume, triplicando el consumo de un canal no seguro.

Se evidencia que el incremento en el consumo de energía introducido por la compresión es proporcionalmente bajo en relación a la mejora de throughput alcanzada. Esto hace, que la compresión sea una opción a considerar en escenarios donde se requiera mejorar el rendimiento del ancho de banda y la energía no sea un factor critico.

Observamos que el protocolo IPSec consigue un mejor aprovechamiento del ancho de banda y menor consumo de energía, comparado con el protocolo SSL/TLS sin compresión.

El uso de canal seguro en lugar de un canal no seguro, introduce una disminución en el rendimiento del ancho de banda (entre un 10% y 20%) y un incremento en el consumo de energía (entre un 100% y 200%). La elección de un nivel de seguridad en los nodos ad hoc dependerá de las posibilidades de recarga de energía y del ancho de banda disponible en la zona de despliegue de la MANET.

Para continuar con esta línea de investigación tenemos previsto:

- Utilizar dispositivos con interfaces Bluetooth 4.0 de bajo consumo.
- Efectuar pruebas variando la potencia de transmisión del nodo cliente y la distancia entre el nodo cliente y el nodo Gateway.
- Incorporar compresión DEFLATE al protocolo IPSEC y comparar los resultados con los obtenidos para la compresión LZO.
- Utilizar herramientas de simulación para modelar el comportamiento aleatorio y la congestión de la red GPRS.
- Estudiar la distribución del consumo de energía entre los componentes de un protocolo seguro: Intercambio de claves, autenticación, integridad, encriptación y transmisión de datos.

Referencias

1 IETF. *MANET Active Work Group*. http://tools.ietf.org/wg/manet

2 CORDEIRO DE MORAIS, Carlos and AGRAWALL Dharma. (2011). Integrating MANETs, WLANs and Cellular Networks. In World Scientific Publishing (Ed.), *Ad Hoc and Sensor Networks - Theory and Applications* (pp. 587-620). Singapore: World Scientific Publishing.

3 ROCABADO, Sergio; SANCHEZ, Ernesto; DIAZ, Javier y ARIAS FIGUEROA, Daniel. (2011). *Integración Segura de MANETs con Limitaciones de Energía a Redes de Infraestructura*. Paper presented at the CACIC 2011, La Plata - Buenos Aires - Argentina. http://sedici.unlp.edu.ar/handle/10915/18771

4 ROCABADO, Sergio; SANCHEZ, Ernesto; DIAZ, Javier y ARIAS FIGUEROA, Daniel. (2012). *Integración Segura de MANETs, desplegadas en zonas de recursos*

limitados, a Redes de Infraestructura. Paper presented at the CACIC 2012, Bahia Blanca - Buenos Aires - Argentina. http://sedici.unlp.edu.ar/handle/10915/23762

5 ROCABADO, Sergio; HERRERA, Susana y Otros. (2013). *M-LEARNING EN ZONAS DE RECURSOS LIMITADOS*. Paper presented at the TE&ET 2013, Santiago del Estero - Argentina.

6 CORDEIRO DE MORAIS, Carlos and AGRAWALL Dharma. (2011). Wireless PANs. In World Scientific Publishing (Ed.), *Ad Hoc and Sensor Networks - Theory and Applications* (pp. 196-258). Singapore: World Scientific Publishing.

7 SPECIAL INTEREST GROUP (SIG) Bluetooth. (2001). Specification of the Bluetooth System, tomo 2. *Bluetooth Profiles Specification Version 1.1*.

8 ETSI EN 301 344. (2000). *Digital cellular telecommunications system, General Packet Radio Service (GPRS), Service description*. Retrieved from http://www.etsi.org/index.php/technologies-clusters/technologies/mobile/gprs

9 SPECIAL INTEREST GROUP (SIG) Bluetooth. (2001). Bluetooth Network Encapsulation Protocol (BNEP) Especification.

10 3GPP. (2011). Specification 29060 - GPRS Tunneling Protocol, release 11.0. from http://www.3gpp.org/ftp/Specs/html-info/SpecVsWi--29060.htm

11 STERICSON, Stephen. (2011). BusyBox. from https://play.google.com/store/apps/details?id=stericson.busybox

12 FOLKERT van Heusden. HTTPing for Google Android mobile phones. Retrieved from http://www.vanheusden.com/Android/HTTPing

13 MAGICANDROIDAPPS.COM. (2011). Iperf for Android. from https://play.google.com/store/apps/details?id=com.magicandroidapps.iperf

14 GORDON, Mark; ZHANG, Lide and TIWANA, Birjodh. PowerTutor. University of Michigan. Retrieved from http://ziyang.eecs.umich.edu/projects/powertutor

15 SCHÄUFFELHUT, Friedrich. OpenVPN Installer. Retrieved from http://code.google.com/p/android-openvpn-installer

16 OpenVPN for Windows. (2010). from http://openvpn.net/index.php/download.html

17 PATEL, B.; ABOBA, B y Otros (2001). *L2TP/IPsec, RFC 3193*. IETF. Retrieved from http://tools.ietf.org/html/rfc3193

18 DIERKS, T.; RESCORLA, E. (2008). *The Transport Layer Security (TLS) Protocol (ver 1.2)*. IETF. Retrieved from http://tools.ietf.org/html/rfc5246

19 OBERHUMER, Markus F.X.J. (2010). LZO compression. from http://www.oberhumer.com/opensource/lzo/

20 ZHANG, Lide; TIWANA, Birjodh; QIAN, Zhiyun and WANG, Zhaoguang. (2010). *Accurate online power estimation and automatic battery behavior based power model generation for smartphones*. Paper presented at the 2010 IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Scottsdale, AZ. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5751489